REMARKS

Claims 1-2, 4-7, 9-16 and 22-25 are pending in the application.

Independent claims 1, 22, and 24 are each amended above (a) to clarify the nature of the security threats and (b) to introduce a firewall or data diode before the format converter: claim 23 is made dependent upon claim 22.

Claim 3 has been amended to correct a typographical error.

Claim 7 is amended to correct dependencies.

Claim 11 has been cancelled.

New claim 25 is directed to a method wherein data diodes, are located both before and after the format converter.

No new matter has been added to the application by way of these specification and claim amendments.

I. THE CLAIM 7 OBJECTION

The examiner objected to claim 7 because it depends upon a cancelled claim.

The examiner's objection has been overcome by amending claim 7 to depend upon claim 1.

II. THE SECTION 112, 2nd PARAGRAPH REJECTION OF CLAIMS 15 AND 16

The examiner rejected claims 15 and 16 for being indefinite owing to an alleged conflict between the wording of claim 1 – "wherein a security domain comprises a network having a common level of resilience to security threats" and that of claims 15 and 16 which stipulate that the security domains be of different security levels.

The examiner's rejection is overcome by amending claim 1 to more clearly indicate that it is the network forming a given individual security domain which exhibits a commonality of resilience within and across that given security domain to security threats. Therefore is quite possible for two security domains, each of which individually comprises a network exhibiting a common resilience within that network to security threats, to exhibit different levels of resilience.

III. THE OBVIOUSNESS REJECTION

The examiner rejected claims 1-5, 7-16, and 22-24 for being obvious over Patton in view of a variety of secondary references. The pending and amended application claims are non-obvious and patentable over the cited prior art for at least the reasons recited below.

The presently claimed invention is directed to a computerized method of removing *covert* (i.e. hidden or concealed) threats from a document, whereas the security threats disclosed in Patton et al. (a) are all *overt* threats in the form of sensitive data plainly visible within the document in normal use and (b) also do not include either malicious code (claims 1, 22, 24) or data steganographically concealed within the document (claim 13). Consequently the disclosure of Patton fails even to disclose the problem addressed by the present invention, namely dealing with malicious code security threats covertly located in documents.

Furthermore Patton et al. fails to disclose the use of a firewall or data diode either before the reformatter (claims 1, 22, 24) or both before and after the reformatter (claims 4, 25). Contrary to Examiner's argument Patton makes no disclosure of either a firewall or a data diode: neither term nor structure is used at Examiner's cited reference of paragraph 31 of Patton et al. nor is any system described which would describe such an arrangement. Instead, Patton makes reference only to shipping by "US Government export control license or company or organizational arrangements" none of which suggests the functionality of either a computer firewall or data diode. Particularly with respect to the data diode (claims 1, 4, 22, 24, and 25) none of the methods described in paragraph 31 even suggest prevent information flow in the reverse direction, contrary to the key functionality of a data diode.

It is also evident that the teaching of Patton et al. is expressly to amend the visible informational content (see for example Figures 7-9) which teaches directly away from present claim 5.

Consequently the skilled person would not be led to begin from Patton et al. to address the present problem.

In view of the above, Examiners' combination of Patton with Simard is considered moot. Nevertheless it may be noted that regarding claims 1, 22, 23, and 24 the disclosure of Simard et al. fails to make good the shortfalls in disclosure evident in Patton et al. so that even in the unlikely event that the skilled person were to consider Patton in view of Simard he could not arrive at the present invention without inventive step.

Neither the disclosure of Carter nor that of Walsh serves to make good the deficiencies in disclosure of Patton et al. and the disclosure of Walsh, as applied by Examiner, merely serves to confirm that certain malicious code threats exist.

CONCLUSION

All pending application claims are believed to be ready for patenting for at least the reasons recited above. Favorable reconsideration and allowance of all pending application claims is, therefore, courteously solicited.

McDonnell Boehnen Hulbert & Berghoff LLP

Date: June 30, 2011

By: ___/A. Blair Hughes/________________
A. Blair Hughes
Reg. No. 32,901